The claims have been amended to overcome the outstanding § 101 rejection, and to better define the invention generally, without narrowing the scope of the claims. Among other things, the default input password has been changed to the more descriptive term "general access password." The specification has been amended to relate the two terms to each other.

The claims have also been amended to better define the invention. With the present invention, a first user can obtain access by providing a password. If desired, the first user can access the information without entering the password, to reduce a frequency of entering the password, by making the general access password the password. Entering the password for every access is troublesome for the first user when the first user accesses the information continuously. According to this invention, the first user can selectively validate or invalidate the access control on a use scene without changing the password for access control, by only changing the general access password.

Also, the first user can permit a second user to access the information, by making a general access password the password. The first user can deny the second user access to the information by making the general access password different from the password. In this manner, the first user can selectively allow the second user to access the information without disclosure of the password to the second user.

Claims 1-2, 5 and 18 stand rejected under § 103 on the basis of Rupp Corporation. Applicants respectfully traverse this rejection because Rupp does not disclose or suggest the password preserving unit or the password verifying unit of the claimed

invention. At most, Rupp suggests ideas or concepts about a default password, without providing an enabling disclosure. Rupp is, after all, merely a sales announcement.

Claims 1-2, 5 and 18 stand rejected under § 103 on the basis of Hideo (JP 62-9471). Applicants respectfully traverse this rejection because Hideo does not disclose (or suggest) a storage apparatus in which a general access password can be used to allow essentially free access to the storage apparatus by a first or second user, as in the present invention.

For the foregoing reasons, applicants believe that this case is in condition for allowance, which is respectfully requested. The examiner should call applicants' attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns
Registration No. 29,367

May 16, 2002

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Facsimile: 312.360.9315
F:\DATA\WP60\1990\62597\Amend A.doc

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Specification:

The paragraph beginning on page 4, line 2 was amended as follows:

According to the invention, a storing apparatus for protecting an access of information recorded on a medium by a password has a password preserving unit and a password verifying unit. The password preserving unit preserves a general access (default) input password and a password for access protection. When there is no password input from the user, the password verifying unit substitutes the default input password for the user input password and compares and collates the default input password with the password for access protection, thereby controlling the access protection. When there is a password input by the user, the user input password and the password for access protection are compares and collated, thereby controlling the access protection. Especially, when the password preserving unit preserves the same value as a default input password and a password for access protection, even if there is no password input by the user, the password verifying unit substitutes the default input password for the user input password and collates the default input password with the password for access protection, thereby permitting the access. According to the invention as mentioned above, when the default input password is stored on the storing apparatus side and there is no password input from the user, the password

verification is performed by regarding the default input password as a user input password. Consequently, by setting the default input password and the password for access protection to the same value, even when the user does not input the password, the access is permitted and an access by an ordinary command can be performed and the password input by the user can be omitted.

The paragraph beginning on page 13, line 24 was amended as follows:

Fig. 1 is a block diagram of a hard disk drive (HDD) to which a password protection using a general access (default) input password of the invention is applied. In the hard disk drive, a magnetic disk medium is fixedly built in a drive main body. The hard disk drive is constructed by an enclosure 10 and a control board 12. The enclosure 10 has a head IC circuit 14 and four head assemblies 16-1 to 16-4 are connected thereto in the embodiment. Each of the head assemblies 16-1 to 16-4 has a recording head using an inductive head and a reproducing head using an MR head or the like. The enclosure 10 also has a VCM 18 for driving a head actuator and a spindle motor 20 for rotating a disk medium. For the head IC circuit 14 in the enclosure 10, a write channel circuit 28 and a read channel circuit 26 are provided on the control board 12 side. A hard disk controller 24 is provided for the write channel circuit 28 and the read channel circuit 26. A formatter, an ECC circuit, and the like are built in the hard disk controller 24. The hard disk controller 24 is connected to an

interface circuit 36. The supply of write data from a host serving as an upper apparatus and the transfer of read data to the host are executed by a data transmission from/to the host side. As an interface circuit 36, a proper interface such as SCSI interface, ATA interface, ATAPI interface, SCSI, or the like can be used. In the embodiment, a constant density recording system (ZCDR) by a zone division is used as a recording system of a disk medium. Cylinders of the disk medium are divided into zones every predetermined number of cylinders and different frequencies have been preset for respective zones. For this purpose, a PLL circuit 30 functioning as a frequency synthesizer is provided. By setting a corresponding zone frequency from a cylinder address upon reading or writing operation, clocks are supplied to the write channel circuit 28 and read channel circuit 26. The whole control of the hard disk drive is performed by an MCU (main control unit) 22. The hard disk controller 24 and interface circuit 36 are connected to the MCU 22 via a bus and, further, an RAM 38 functioning as a work memory and a flash ROM 40 functioning as a non-volatile memory are connected. The MCU 22 receives and decodes various commands from the host, instructs the hard disk drive to perform an ordinary reading or writing operation by an ordinary command, and instructs a servo controller 34 to execute a head positioning control by the VCM 18 provided for the enclosure 10. In order to execute the head positioning control by the driving of the VCM 18, a servo demodulating circuit 32 and the servo controller 34 are provided. In the embodiment,

as servo information of the disk medium, a data surface servo system is used. Therefore, servo information is separated from a reproduction signal for the read channel circuit 26 and head position information is reconstructed by the servo demodulating circuit 32.

In the Claims:

Claims 1-9, 11, 12, 15-17, 19 and 21 were amended as follows:

1. (Amended) A storing apparatus ~~for protecting an access of~~ in which a first user can protect access to information recorded on a medium ~~by~~with a password, and can selectively permit said first user and a second user to access the information without the password, comprising:

a password preserving unit for preserving a ~~default~~ general access ~~input~~ password and a~~t~~he password ~~for access protection~~; and

a password verifying unit for ~~controlling the access protection by substituting said default input password for a user input password and comparison collating with said password for access protection when there is not password input from the user and for controlling the access protection by comparison collating the user input password with said password for access protection when there is the password input from the user.~~allowing access if the password is entered, and if the password is not entered, comparing the general

access password with the password, allowing access if the general access password is the password, and denying access if the general access password is not the password.

2. (Amended) An apparatus according to claim 1, wherein in the case where a same value has been preserved in the general access~~said default input~~ password and the~~said~~ password for access protection by said password preserving unit, even if there is no user input password input by the user, said password verifying unit permits an access by substituting said general access~~default input~~ password for the user input password and comparing the general access password~~collating~~ with the password for access protection.

3. (Amended) An apparatus according to claim 1, wherein

said password preserving unit further has a user input password area to store a~~the~~ user input password input by a user, and

said password verifying unit is constructed in a manner such that

at the start of the use of the apparatus such as turn-on of a power source, command reset, error reset, ~~further,~~ medium insertion, or the like, said general access~~default input~~ password is read out and written into said user input password area, an access permission is established if the general password is the password, or an access inhibition is

established if the general password is not the password,~~an access permission or inhibition is subsequently established~~ on the basis of a collation ~~coincidence~~ between the general access password in said user input password area and the~~said~~ password for access protection,

after said~~the~~ access permission or inhibition is ~~was~~ established, each time there is a password input of the user, the user input password is written into said user input password area and, subsequently, the access permission inhibition is established on the basis of a collation ~~coincidence~~ between the user input password in said user input password area and the~~said~~ password for access protection.

4. (Amended) An apparatus according to claim 1, wherein

said password preserving unit further has a user input password area to store a~~the~~ user input password input by a user, and

said password verifying unit is constructed in a manner such that

at the start of the use of the apparatus such as turn-on of a power source, command reset, error reset, ~~further,~~ medium insertion, or the like, the apparatus waits for the password input by the user in a state where said general access~~default input~~ password is read out and written into said user input password area,

when there is the user password input, the user input password is overwritten into the general access ~~default input~~ password in said user input password area,

and after that, the password in said user input password area and said password for access protection are ~~collated and~~ compared and the access protection is controlled, and

when there is no user password input and/or in the case where the password is an empty character train even if there is the user password input, the ~~collation~~ comparison between the general access ~~default input~~ password in said user input password area and the~~said~~ password for access protection is executed and the access protection is controlled.

5. (Amended) An apparatus according to claim 1, wherein said password preserving unit preserves said general access ~~default input~~ password and said password for access protection into a non-volatile memory of an apparatus main body.

6. (Amended) An apparatus according to claim 1, wherein

said password preserving unit preserves said general access ~~default input~~ password and said password for access protection into said medium, and

said password verifying unit reads out said general access~~default input~~ password and said password for access protection from said medium and stores into an apparatus main body at the start of the use of the apparatus and controls the access protection.

7. (Amended) An apparatus according to claim 1, wherein

said password preserving unit preserves said general access~~default input~~ password into a non-volatile memory of an apparatus main body and preserves said password for access protection into the medium, and

said password verifying unit reads out said password for access protection from said medium and stores into the apparatus main body at the start of the use of the apparatus and controls the access protection.

8. (Amended) An apparatus according to claim 1, wherein

said password preserving~~verifying~~ unit preserves said password for access protection into a non-volatile memory of an apparatus main body and preserves said general access~~default input~~ password into the medium, and

said~~a~~ password verifying~~processing~~ unit reads out said general access~~default input~~ password from said medium and stores into the apparatus main body at the start of the use of the apparatus and controls the access protection.

9. (Amended) An apparatus according to claim 1~~anyone of claims 5 to 7~~, wherein in said medium, a password preserving area to preserve said password is provided in a specific area which cannot be accessed by an ordinary read command and write command.

11. (Amended) An apparatus according to claim 1~~anyone of claims 5 to 7~~, wherein said medium is a medium fixedly enclosed in the apparatus main body.

12. (Amended) An apparatus according to claim 1~~anyone of claims 5 to 7~~, wherein said medium is a removable medium which is detachable from~~for~~ the apparatus main body.

15. (Amended) An apparatus according to claim 1, further comprising a validity term setting unit for setting a validity term into said general access~~default input~~ password.

16. (Amended) An apparatus according to claim 15, wherein said validity term setting unit counts the number of using times of the apparatus by a counter and, when a value of said counter reaches a predetermined value, said validity term setting unit forcedly changes said general access~~default input~~ password to a value different from the general access~~default~~ password so far.

17. (Amended) An apparatus according to claim 15, wherein said validity term setting unit sets a time of a validity term and, when a present time in case of using the

apparatus exceeds said validity term, said validity term setting unit forcedly changes said general access~~default input~~ password to a value different from the general access~~default~~ password so far.

19. (Amended) A method according to claim 18, wherein in the case where a same value has been preserved in said general access~~default input~~ password and said password for access protection, in said password verifying step, prior to the password input of the user, a value of said general access~~default input~~ password is copied to the user input password and is collated with said password for access protection, thereby permitting or inhibiting an access.

21. (Amended) A method according to claim 18, further comprising a validity term setting step of setting a validity term into said general access~~default input~~ password.